

UNITED STATES DISTRICT COURT
 for the
 Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
 or identify the person by name and address)*

)
)
)

Case No. 3:21MJ394

INFORMATION ASSOCIATED WITH NICKELJRD71@GMAIL.COM

AND DONALDDNICKELLJR@GMAIL.COM THAT IS STORED AT

PREMISES CONTROLLED BY GOOGLE

)
)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See attachment A

located in the Southern District of Ohio, there is now concealed (*identify the person or describe the property to be seized*):

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

See attachment C

The application is based on these facts:

See attached affidavit of SA Kimberly Wallace

Continued on the attached sheet.

Delayed notice of days (*give exact ending date if more than 30 days: _____*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

KIMBERLY A WALLACE

Digitally signed by KIMBERLY A WALLACE
 Date: 2021.11.01 16:01:14 -04'00'

Applicant's signature

SA Kimberly Wallace, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Facetime

(specify reliable electronic means).

Date: 11/02/2021



Judge's signature

Hon. Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

City and state: Dayton, Ohio

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with NICKELEJRD71@GMAIL.COM and DONALDDNICKELLJR@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Ampitheater Parkway, Mountainview, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 17, 2021 (Google case number 6412324), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the accounts from December 23, 2017 until present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, those violations involving Donald Darrell Nickell and occurring after December 23, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Child pornography, obscene materials involving children, pictures of children, communications with children;
- (b) Communications with others about sexual interest in children, child pornography, obscene materials involving children, sexual acts involving children, sexual exploitation of children;
- (c) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (d) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (f) The identity of the person(s) who communicated with the user ID about matters relating to child pornography and child exploitation, including records that help reveal their whereabouts.

III. Method of delivery

Notwithstanding 18 U.S.C. § 2252, Google may disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System (LERS) to Homeland Security Investigations Special Agent Kimberly Wallace (kimberly.a.wallace@lers.google).

ATTACHMENT C

<u>Code Section</u>	<u>Offense Description</u>
<u>18 U.S.C. §2252(a)(4)(B) & (b)(1)</u>	Possession of Child Pornography
<u>18 U.S.C. §2252A(a)(5)(B) & (b)(1)</u>	Possession of Child Pornography
<u>18 U.S.C. §2252(a)(2)(B) & (b)(1)</u>	Receipt and Distribution of Child Pornography
<u>18 U.S.C. §2252A(a)(2) & (b)(1)</u>	Receipt and Distribution of Child Pornography

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
NICKELJRD71@GMAIL.COM AND
DONALDDNICKELLJR@GMAIL.COM
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Kimberly Wallace, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, an email provider headquartered at 1600 Ampitheater Parkway, Mountainview, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”), and have been since June 2010. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C.

§§ 2251(a) and (e), 2252(a), and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252 and 2252A have been committed by Donald Darrell Nickell. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND ON NCMEC

6. The National Center for Missing and Exploited Children (NCMEC), among other things, tracks missing and exploited children and serves as a repository for information about child pornography. Companies that suspect that child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip. To make such a report, a

company providing services on the internet, electronic service providers (“ESPs”) and internet service providers (“ISPs”), can go to an online portal that NCMEC has set up for the submission of these tips. The ISP or ESP then can provide to NCMEC information concerning the child exploitation activity it believes to have occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. The ISP or ESP may also upload to NCMEC any files it collected in connection with the activity. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP or ESP provides, such as IP addresses. NCMEC then packages the information from the ISP and ESP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

FACTS SUPPORTING PROBABLE CAUSE

7. In August 2021, HSI Attaché Rome received information from Italian law enforcement regarding an Italian citizen who received emails which contained child pornography. Email accounts NICKELJRD71@GMAIL.COM (“**SUBJECT ACCOUNT-1**”) and DONALDDNICKELLJR@GMAIL.COM (“**SUBJECT ACCOUNT-2**”) had sent the Italian citizen several email attachments which depicted child pornography.

a. On or about August 15, 2020, **SUBJECT ACCOUNT-1** sent a message with the subject line of “girls” and contained six (6) attachments. I reviewed the email and attachments, which HSI Attaché Rome had forwarded to investigators in the United States. Based on my review, I found images in the attachments that contained child pornography, including:

- i) The image with filename, “2_5efe487d7c7f3”, depicted a prepubescent child leaning back on their elbow with their clothing pulled down below their chest. A hand is holding an adult male’s penis and is placing the penis in the child’s mouth while another hand holds the back of the child’s head. Based on my training and experience, I believe that this image depicts child pornography.
- ii) The image with filename, “2q3wk9d5.jpg”, depicted an adult male’s penis inserted into the vagina of an unconscious female toddler. Based on my training and experience, I believe that this image depicts child pornography.

b. On or about August 15, 2020, **SUBJECT ACCOUNT-2** sent a message with the subject line of “girls” and contained five (5) attachments. I reviewed the email and attachments, which HSI Attaché Rome had forwarded to investigators in the United States. Based on my review, I found images in the attachments that contained child pornography, including:

- i) The image with filename, “2+(1).jpg”¹, depicted a nude prepubescent female performing fellatio on a pubescent male with the female’s legs spread open. Based on my training and experience, I believe that this image depicts child pornography.

¹ Email correspondence reflected a filename of “2 (1).jpg” while the image HSI received from Italian law enforcement authorities reflected a filename of “2+(1).jpg”. On or about September 30, 2021, Italian authorities confirmed that the image was the exact same file.

8. On or about August 13, 2021, administrative summons' were issued to Google for subscriber and IP address information for **SUBJECT ACCOUNT-1** and **SUBJECT ACCOUNT-2**.

2. Google responded with the following subscriber information:

- a. Google Account ID: 564192839240
- b. Name: DONALD D NICKELL JR
- c. Given Name: DONALD D
- d. Family Name: NICKELL JR
- e. e-Mail: donalddnickelljr@gmail.com
- f. Recovery SMS: +19373601056 [US]
- g. Login: 2020-11-10 21:36:42 UTC 2605:a000:1307:a4d6:b538:8405:8c8:c069
- h. Google Account ID: 21017430864
- i. Name: Donald D Nickel Jr
- j. Given Name: Donald D
- k. Family Name: Nickel Jr
- l. e-Mail: nickeljrd71@gmail.com
- m. Recovery SMS: +19373601056 [US]
- n. Login: 2021-07-25 21:30:05 UTC 2603:6010:ae01:25d5:3ca1:c75e:c51c:630

9. In August 2021, HSI Cincinnati received the above-referenced information. On or about August 16, 2021, an administrative summons was issued to Charter Communications for IP address 2603:6010:ae01:25d5:3ca1:c75e:c51c:630 for 07/25/2021 at 21:30:05 UTC and for IP address 2605:a000:1307:a4d6:b538:8405:8c8:c069 for 11/10/2020 at 21:36:42 UTC. Charter responded with the following subscriber information for both IP addresses:

Subscriber Name:	Darrel Nickell ²
Service Address:	1707 E HIGH ST, APT 608, SPRINGFIELD, OH 45505-1289
User Name or Features:	SUBJECT ACCOUNT-1
Phone number:	(937) 360-1056

10. Multiple NCMEC CyberTipline Reports were associated with **SUBJECT ACCOUNT-1**. On or about August 16, 2021, HSI Cincinnati requested copies of the NCMEC reports and attachments from the Ohio Internet Crimes Against Children Task Force.

CyberTipline Report 77020524

11. On or about August 19, 2020, NCMEC received a report from Oath Holdings, Inc. (“Oath”), an ESP. Oath classified the incident type as child pornography and the files were transmitted over Yahoo Mail. The CyberTipline Report identified the suspect account with a name of “Dawn Jones”, with a cell phone number of 937-360-1056³, and an email address of dawnj43@yahoo.com. The CyberTipline Report included six (6) uploaded files for the reported account. All files were viewed by the ESP.

- a. I viewed the file named image.2-1.jpeg, and it is an image of a prepubescent child with an adult male’s penis in their mouth and the child’s hand is holding the

² Based on my investigation, and my training and experience, I believe that the subscriber identified as “Darrel Nickell” is Donald Darrell NICKELL and Charter Communications’ utilized NICKELL’s middle name as a first name. My belief is based on additional record queries to include OHLEG, public records, and subscriber information as described below which included multiple sources identifying NICKELL as the subscriber of telephone number (937) 360-1056 and the resident of 1707 E High St, Apt 608, Ohio 45505. Additionally, the telephone number listed on Charter’s subscriber information is the same number listed in Google subscriber information.

³ The telephone number was listed in subscriber information for google target accounts and in subscriber information for IP addresses utilized by the google target accounts.

penis. Based on my training and experience, I believe that this image depicts child pornography.

- b. I viewed the file named image.3-1.jpeg, and it is an image of a prepubescent female straddling an adult male with his penis inserted into her vagina. The female is wearing a pink mask and has the words “CUMDUMP” and “FUCK ME” with an arrow pointing downward written on her chest and abdomen. Based on my training and experience, I believe that this image depicts child pornography.
- c. I viewed the file named image.4-1.jpeg, and it is an image of a nude prepubescent female with an adult male’s penis in her mouth and both of her hands are holding the penis. Based on my training and experience, I believe that this image depicts child pornography.

CyberTipline Report 77023460

12. On or about August 19, 2020, NCMEC received a report from Oath, an ESP. Oath classified the incident type as child pornography and the files were transmitted over Yahoo Mail. The CyberTipline Report identified the suspect account with a name of “dawn jones”, with a cell phone number of 937-360-1056⁴, and an email address of dawnjones656@yahoo.com. The CyberTipline Report included four (4) uploaded files for the reported account. All files were viewed by the ESP.

- a. I viewed the file named image.1-1.jpeg, and it is an image of a prepubescent child with an adult male’s penis in their mouth and the child’s hand is holding the

⁴ The telephone number was listed in subscriber information for the google target accounts and in subscriber information for IP addresses utilized by the google target accounts.

penis. The image appeared to be the same image as referenced in the previous section for CyberTipline 77020524 for image.2-1.jpeg. Based on my training and experience, I believe that this image depicts child pornography.

- b. I viewed the file named image.3-1.jpeg, and it is an image of a prepubescent female straddling an adult male with his penis inserted into her vagina. The female is wearing a pink mask and has the words “CUMDUMP” and “FUCK ME” with an arrow pointing downward written on her chest and abdomen. The image appeared to be the same image as referenced in the previous section for CyberTipline 77020524 for image.3-1.jpeg. Based on my training and experience, I believe that this image depicts child pornography.
- c. I viewed the file named image.5-1.jpeg, and it is an image of a nude prepubescent female with an adult male’s penis in her mouth and both of her hands are holding the penis. The image appeared to be the same image as referenced in the previous section for CyberTipline 77020524 for image.4-1.jpeg. Based on my training and experience, I believe that this image depicts child pornography.

CyberTipline Report 77047422

13. On or about August 19, 2020, NCMEC received a report from Oath, an ESP. Oath classified the incident type as child pornography and the files were transmitted over Yahoo Mail. The CyberTipline Report identified the suspect account with a name of “darrell nickell”, with a cell phone number of 937-360-1056⁵, and an email address of darrellnickell@yahoo.com. The

⁵ The telephone number was listed in subscriber information for the google target accounts and in subscriber information for IP addresses utilized by the google target accounts.

CyberTipline Report included four (4) uploaded files for the reported account. All files were viewed by the ESP.

- a. I viewed the file named image.1-1.jpeg, and it is an image of a prepubescent child with an adult male's penis in their mouth and the child's hand is holding the penis. The image appeared to be the same image as referenced in the previous section for CyberTipline 77020524 for image.2-1.jpeg. Based on my training and experience, I believe that this image depicts child pornography.
- b. I viewed the file named image.2-1.jpeg, and it is an image of a prepubescent female straddling an adult male with his penis inserted into her vagina. The female is wearing a pink mask and has the words "CUMDUMP" and "FUCK ME" with an arrow pointing downward written on her chest and abdomen. The image appeared to be the same image as referenced in the previous section for CyberTipline 77020524 for image.3-1.jpeg. Based on my training and experience, I believe that this image depicts child pornography.
- c. I viewed the file named image.3-1.jpeg, and it is an image of a nude prepubescent female straddling a nude pubescent-aged female in shallow water with the pubescent-aged female putting her finger into the vagina of the prepubescent female. Based on my training and experience, I believe that this image depicts child pornography.
- d. I viewed the file named image.4-1.jpeg, and it is an image of a pubescent-aged male putting his finger into the vagina of a prepubescent female while the prepubescent female is sitting with her legs open and her arms/hands behind bracing herself.

Based on my training and experience, I believe that this image depicts child pornography.

CyberTipline Report 77592730

14. On or about August 24, 2020, NCMEC received a report from Yahoo, Inc (Verizon Media), an ESP. The report was classified as a supplemental report to CyberTipline Reports 77047422, 77020524, and 77023460 (as referenced in the previous three sections). The report included additional information utilized for the target Yahoo accounts.

- a. Account darrellnickell@yahoo.com provided a date of birth of [REDACTED] (Nickell's actual date of birth) and the telephone number 937-360-1056 which was verified on 08/18/2020. The account was created on 08/18/2020 at 20:43:27 (GMT) from IP address 2605:a000:1307:84ea:9d15:213e:18e7:4a0a.
- b. Account dawnj43@yahoo.com provided a date of birth of [REDACTED] and the telephone number 937-360-1056 which was verified on 08/17/2020. The last successful login for the account was on 08/18/2020 at 17:24:02 (GMT) from IP address 2605:a000:1307:84ea:9d15:213e:18e7:4a0a.
- c. Account dawnjones656@yahoo.com provided a date of birth of [REDACTED] and the telephone number 937-360-1056 which was verified on 08/16/2020. The last successful login for the account was on 08/18/2020 at 17:33:02 (GMT) from IP address 2605:a000:1307:84ea:9d15:213e:18e7:4a0a. An alternate email address provided was **SUBJECT ACCOUNT-1**.
- d. Telephone number 937-360-1056 was associated with another account of nickeljrd71@yahoo.com. The telephone number was verified on 08/18/2020 and an alternate email address provided was **SUBJECT ACCOUNT-1**. The date of

birth provided for the account was [REDACTED] (Nickell's actual date of birth) and the last successful login for the account was on 08/18/2020 at 20:19:31 (GMT) from IP address 2605:a000:1307:84ea:9d15:213e:18e7:4a0a.

i. On or about August 17, 2021, an administrative summons was served upon Charter Communications for 08/18/2020 from 18:09:11 to 20:19:31 UTC for IP address 2605:a000:1307:84ea:9d15:213e:18e7:4a0a. Charter responded with the following:

Subscriber Name:	Darrel Nickell
Service Address:	1707 E HIGH ST, APT 608, SPRINGFIELD, OH 455051289
Billing Address:	1707 E HIGH ST, APT 608, SPRINGFIELD, OH 455051289
User Name or Features:	SUBJECT ACCOUNT-1
Phone number:	(937) 360-1056

Record Queries and Summons

15. On or about August 27, 2021, an administrative summons was issued to Q Link Wireless LLC for subscriber information for telephone number 937-360-1056. Q Link Wireless responded with the following:

- a. Name: Donald Nickell Jr
- b. Date of Birth: [REDACTED]
- c. Last 4 of SSN: [REDACTED]
- d. Address: 1707 E HIGH ST, APT 608, SPRINGFIELD, OH 45505-1289 US
- e. Email: **SUBJECT ACCOUNT-1**

16. On or about September 13, 2021, an Ohio Law Enforcement Gateway (OHLEG) query for Nickell revealed a valid Ohio driver's license for Donald D Nickell Jr. Nickell (██████████ listed 1707 E High St, Apt 608, Springfield, Ohio as his residence on his driver's license. The license was issued on March 3, 2021.

17. OHLEG revealed an Electronic Sex Offender Registration and Notification (eSorn) for Donald Darrell Nickell (██████████ which was inactive/expired. The compliance period reflected a 10-year requirement.

18. A criminal history query for Nickell revealed that Nickell had been convicted in Springfield, OH of four (4) counts of gross sexual imposition with the victim being under the age of 13.

19. On or about October 8, 2021, an administrative summons was issued to Hugh Taylor Apartments for current occupant information for 1707 E High St, Apt 608, Springfield, OH 45505. The following pertinent information was received:

- a. Applicant information for Donald D Nickell Jr, listed contact information of 937-360-1056 (cell) and **SUBJECT ACCOUNT-1** which was signed by Nickell on 03/25/2020.
- b. A copy of an Ohio driver's license for Nickell was included in the documentation which matched the current driver's license number (██████████ for Nickell.
- c. A State of Ohio (Clark County) judgment entry of conviction for Nickell (05-CR-366) was included which reflected a sentence of five years community control and classified Nickell as a sexually oriented offender was dated October 2005. The conviction was for four counts of gross sexual imposition and required Nickell to register as a sex offender for 10 years.

BACKGROUND CONCERNING EMAIL

20. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

21. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

22. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to

identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

23. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the forgoing, there is probable cause to believe that the NICKELEJRD71@GMAIL.COM and DONALDDNICKELLJR@GMAIL.COM accounts contain evidence, instrumentalities, contraband, and/or fruits of crimes including possession, receipt, and distribution of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I therefore respectfully request that the Court issue the proposed search warrant.

//

//

//

//

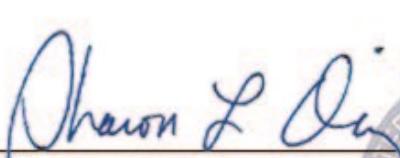
28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

KIMBERLY A WALLACE 
Digitally signed by KIMBERLY A WALLACE
Date: 2021.11.01 16:02:44 -04'00'

Kimberly Wallace
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me via Facetime on November 2nd, 2021.


Sharon L. Ovington
United States Magistrate Judge

